Notice of Allowability	Application No. 10/072,331	Applicant(s) MACKENZIE ET AL.	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *5/24/06*.

2. ☒ The allowed claim(s) is/are *1-3 and 5-34*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *7/26/2006*.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
PRIMARY EXAMINER

8/1/06

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William Lewis, Reg. No. 39,274 on 7/26/2006.

1. Replace claims 1,5,6,11,13,14,30 and 33 with the following (shown ***marked up*** here, followed by *clean version*):

1. A method for use in a device associated with a first party for performing a key retrieval operation, the method comprising the steps of:

generating in the first party device a request for

the partial assistance of a device associated with a second party in recovering

a key from

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

transmitting the request from

the first party device to

the second party device;

receiving results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

using at least a portion of the received results in the first party device to

recover the key for subsequent use as a private key in

one or more associated public key cryptographic techniques;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

5. The method of claim 1, wherein

the cryptographic information is generated via

an encryption operation which is a function of

one or more pieces of secret information associated with the first party,

the key, and

a public key associated with the second party device.

6. The method of claim 1, wherein

the results generated by the second party device comprise

results associated with the second party device partially decrypting

at least a portion of the cryptographic information in the request.

11. A method for use in a device associated with a first party for assisting in the performance of a key retrieval operation, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for

the partial assistance of the first party device in recovering

a key from

data stored on the second party device,

wherein

the first party device is remote from

the second party device; and

generating results in the first party device based on

the partial assistance provided thereby for use in the second party device to

recover the key for subsequent use as a private key in

one or more associated public key cryptographic techniques;

wherein

the request generated by the second party device comprises

cryptographic information included in

the data stored on the second party device and

previously generated from the key.

13. Apparatus for use in a device associated with a first party for performing a key retrieval operation, the apparatus comprising:

at least one processor operable to:

(i) generate in the first party device a request for

the partial assistance of a device associated with a second party in recovering

a key from

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

(ii) transmit the request from

the first party device to

the second party device;

(iii) receive results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

(iv) use at least a portion of the received results in the first party device to

recover the key for subsequent use as a private key in

one or more associated public key cryptographic techniques; and

memory, coupled to the at least one processor, for storing

at least a portion of results associated with

one or more operations performed by the processor;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

14. A method for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

generating in the first party device a request for

the partial assistance of a device associated with a second party in performing

a private key operation using a private key associated with

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

transmitting the request from the first party device to the second party device;

receiving results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

using at least a portion of the received results in the first party device

to perform the private key operation;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

30. A method for use in a device associated with a first party for assisting in performing a private key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for

the partial assistance of the first party device in performing

a private key operation using a private key associated with

data stored on the second party device,

wherein

the first party device is remote from

the second party device; and

generating results in the first party device based on

the partial assistance provided thereby for use in the second party device to

perform the private key operation;

wherein

the request generated by the second party device comprises

cryptographic information included in

the data stored on the second party device and

previously generated from the key.

33. Apparatus for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the apparatus comprising:

at least one processor operable to:

(i) generate in the first party device a request for

the partial assistance of a device associated with a second party in performing

a private key operation using a private key associated with

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

(ii) transmit the request from the first party device to the second party device;

(iii) receive results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

(iv) use at least a portion of the received results in the first party device to perform the private key operation; and

memory, coupled to the at least one processor, for storing at least

a portion of results associated with

one or more operations performed by the processor;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

2. Cancel claim 4.

Clean claim version:

1. A method for use in a device associated with a first party for performing a key retrieval operation, the method comprising the steps of:

generating in the first party device a request for

the partial assistance of a device associated with a second party in recovering

a key from

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

transmitting the request from

the first party device to

the second party device;

receiving results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

using at least a portion of the received results in the first party device to

recover the key for subsequent use as a private key in

one or more associated public key cryptographic techniques;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

5. The method of claim 1, wherein

the cryptographic information is generated via

an encryption operation which is a function of

one or more pieces of secret information associated with the first party,

the key, and

a public key associated with the second party device.

6. The method of claim 1, wherein

the results generated by the second party device comprise

results associated with the second party device partially decrypting

at least a portion of the cryptographic information in the request.

11. A method for use in a device associated with a first party for assisting in the performance of a key retrieval operation, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for

the partial assistance of the first party device in recovering

a key from

data stored on the second party device,

wherein

the first party device is remote from

the second party device; and

generating results in the first party device based on

the partial assistance provided thereby for use in the second party device to

recover the key for subsequent use as a private key in

one or more associated public key cryptographic techniques;

wherein

the request generated by the second party device comprises

cryptographic information included in

the data stored on the second party device and

previously generated from the key.

13. Apparatus for use in a device associated with a first party for performing a key retrieval operation, the apparatus comprising:

at least one processor operable to:

(i) generate in the first party device a request for

the partial assistance of a device associated with a second party in recovering

a key from

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

(ii) transmit the request from

the first party device to

the second party device;

(iii) receive results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

(iv) use at least a portion of the received results in the first party device to

recover the key for subsequent use as a private key in

one or more associated public key cryptographic techniques; and

memory, coupled to the at least one processor, for storing

at least a portion of results associated with

one or more operations performed by the processor;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

14. A method for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

generating in the first party device a request for

the partial assistance of a device associated with a second party in performing

a private key operation using a private key associated with

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

transmitting the request from the first party device to the second party device;

receiving results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

using at least a portion of the received results in the first party device

to perform the private key operation;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

30. A method for use in a device associated with a first party for assisting in performing a private key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for

the partial assistance of the first party device in performing

a private key operation using a private key associated with

data stored on the second party device,

wherein

the first party device is remote from

the second party device; and

generating results in the first party device based on

the partial assistance provided thereby for use in the second party device to perform the private key operation;

wherein

the request generated by the second party device comprises cryptographic information included in the data stored on the second party device and previously generated from the key.

33. Apparatus for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the apparatus comprising:

at least one processor operable to:

(i) generate in the first party device a request for the partial assistance of a device associated with a second party in performing a private key operation using a private key associated with data stored on the first party device,

wherein

the second party device is remote from the first party device;

(ii) transmit the request from the first party device to the second party device;

(iii) receive results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

(iv) use at least a portion of the received results in the first party device to perform the private key operation; and

memory, coupled to the at least one processor, for storing at least

a portion of results associated with

one or more operations performed by the processor;

wherein

the request generated by the first party device comprises

cryptographic information included in

the data stored on the first party device and

previously generated from the key.

Examiner's Statement of Reasons for Allowance

3. Claims 1-3,5-34 are allowed over prior art.

4. This action is in reply to applicant's correspondence of 24 May 2006.

5. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

6. As per claims 1,11,13,14,15,30,31,33 and 34 generally, prior art of record, Camp et al, U.S. Patent 6,317,729 B1, fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 5/24/2006 to office action of 2/21/2006.

Specifically, (as per claim 1, for example) prior art dealing with proxy cryptography in general, and cooperating parties engaged in cryptographic services on behalf of another party (i.e., a user), whereas signature and encryption services between network processing elements are typical examples, is generally known to exist per se, (i.e., Ivan, Anca, et al, 'Proxy Cryptography Revisited', Dept. of CS, Courant Inst. of Mathematical Sciences, NY Univ., 2003, entire document, www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/14.pdf). Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the aspect of the first device generating/possessing a stored public encryption private key inaccessible for recovery and subsequent use for '*public key cryptographic techniques*' without the assistance of another external device upon request with the request likewise a function of first device cryptographic information), at the time of the invention; serving to patently distinguish the invention from said prior art;

"1. A method for use in a device associated with a first party for performing a key retrieval operation, the method comprising the steps of:

generating in the first party device a request for

*the partial **assistance** of a device associated with a second party in **recovering***

***a key** from*

*data **stored on the first party device**,*

wherein

the second party device is remote from

the first party device;

transmitting the request from

the first party device to

the second party device;

receiving results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

using** at least a portion of the received results **in the first party device to

***recover the key** for subsequent use as **a private key** in*

one or more associated public key cryptographic techniques;

wherein

the ***request generated** by the first party device* comprises

cryptographic information included in

***the data stored on the first party device** and*

***previously generated from the key**.".*

7. Dependent claims 2,3,5-10,12,16-29 and 32 are allowable by virtue of their dependencies.

Conclusion

8. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
PRIMARY EXAMINER

7/27/06